VERIFICATION OF TRANSLATION

I, the undersigned, Tetsuo AKIYOSHI, residing at 5th Floor, Shintoshicenter Bldg., 24-1, Tsurumaki 1-chome, Tama-shi, Tokyo 206-0034 Japan, hereby certify that to the best of my knowledge and belief the following is a true partial translation into English made by me of Japanese Patent Application No. 2004-197453 filed on July 2, 2004

Dated this 29th day of January, 2007

Tetsuo AKIYOSHI

[Name of Document]	PATENT APPLICATION
[Reference Number]	7048160027
[Filing Date]	July 2, 2004
[To]	Commissioner, Patent Office
[International Patent Classification]	G06F 15/00
[Inventor]	
[Address or Residence]	1006, Oaza Kadoma, Kadoma-shi, Osaka Matsushita Electric Industrial Co. Ltd.
[Name]	Yoshihiko TAKAGI
[Inventor]	
[Address or Residence]	1006, Oaza Kadoma, Kadoma-shi, Osaka Matsushita Electric Industrial Co. Ltd.
[Name]	Takafumi KIKUCHI
[Applicant for Patent]	
[Identification Number]	000005821
[Name]	Matsushita Electric Industrial Co., Ltd.
[Agent]	
[Identification Number]	100105050
[Patent Attorney]	
[Name]	Kimihito WASHIDA
[Declaration of priority based on prior application]	
[Filing Number]	Patent Application No. 2003-275672
[Filing Date]	July 16, 2003
[Indication of Official Fee]	
[Prepayment Register Number]	041243
[Amount of Payment]	¥16,000
[List of Items Submitted]	
[Name of Item]	Scope of Claims 1
[Name of Item]	Specification 1
[Name of Item]	Drawing 1
[Name of Item]	Abstract 1
[Number of General Power of Attorney]	9700376

[0021] According to the invention, by dividing a command for access area designation and a command for security protection area access, and adding verification data to the command for security protection area access, a memory device can verify the identity of a device application having specified the access area, a device application having issued the command for security protection area access, and a device application that holds a verification key shared with a memory card, i.e., having right to access the security protected area. Furthermore, regarding memory access, by using a two-stage command constitution, i.e., a command for access area designation and a command for security protection area access, while command complexity is avoided by using conventional memory card commands, even with only few command argument, without reducing security, access to the security protected area is enabled.

[0023] According to the invention, whether access by a security protected area access command is enabled or disabled can be explicitly set to each area in a security protected area.

[0025] According to the invention, by updating a verification key where needed, security intensity can be enhanced.

[0027] According to the invention, when access is not made to an area where only the device can read and write, access by a security protected area access command can be disabled, and thus security intensity can be enhanced. By updating a verification key where needed, security intensity can be enhanced.

[0029] According to the invention, sharing of information on an accessible area can be divided by command protocol that is different from a command for access area designation and a command for security protection area access, and thus a memory device can verify the identity of a device application having specified the access area, a device application having issued the command for security protection area access, and a device application having right to access the security protected area.

[0031] According to the invention, a verification key sharing process can be divided by command protocol that is different from a command for security protection area access and by updating a verification key restricted to that area, security intensity can be more enhanced.

[0033] According to the invention, an access-enabling setting that is necessary for access to an area with non-tamper resistance is performed by the discretion of a area with tamper-resistance, and read and write of data

are performed using commands suitable for the area with non-tamper resistance, whereby both flexibility of security and read and write performance can be achieved.

[0035] According to the invention, an access-enabling setting that is necessary for access to a area with non-tamper resistance and verification key sharing are performed by the discretion of a area with tamper-resistance, and read and write of data are performed using commands suitable for the area with non-tamper resistance, whereby both flexibility of security and read and write performance can be achieved.

[0037] According to the invention, even when a command for access area designation is different from a command for accessing a memory, it is possible to verify that the two commands are transmitted from the same terminal.

[0038] A tenth invention is directed to a memory device such that in the memory device of the ninth invention the verification process of the designation information verifying section is performed using the verification information and a verification key.

[0039] According to the invention, by using a key, authentication of a terminal using shared secret information with the terminal can be performed.

[0040] An eleventh invention is directed to a memory device such that the memory device of the tenth invention

further comprises verification key sharing section for sharing the verification key with the device.

[0041] According to the invention, by updating a verification key where needed, security intensity can be enhanced.

[0042] A twelfth invention is directed to a memory device such that the memory device of the ninth invention further comprises enabled area information sharing section for sharing enabled area information with the device, the enabled area information indicating an area accessible to the memory device.

[0043] According to the invention, whether access by a security protected area access command is enabled or disabled can be explicitly set to each area in a security protected area.

[0045] According to the invention, data stored in a security protected area of a memory card can be read and written.

[0046] A fourteenth invention is directed to an information device such that in the information device of the thirteenth invention the verification information generation process of the Verification information generating section is performed using the specification information and a verification key.

[0047] According to the invention, by performing verification using a key supplied in secret with a card,

data can be stored in an area where read or write cannot be performed by any other device than the information device.

[0048] A fifteenth invention is directed to an information device such that the information device of the fourteenth invention further comprises a verification key sharing section for sharing the verification key with the memory device.

[0049] According to the invention, by updating a verification key where needed, security intensity can be enhanced.

[0050] A sixteenth invention is directed to an information device such that the information device of the thirteenth invention further comprises an enabled area information sharing section for sharing enabled area information with the memory device, the enabled area information indicating an area accessible to the memory device.

[0051] According to the invention, when access is not made to an area where only the information device can read and write, access by a security protected area access command can be disabled, and thus security intensity can be enhanced.

[0053] According to the invention, by performing verification using a verification key shared between a device and a memory device, access can be allowed only

to the device having right to access.

[0055] According to the invention, by validating access by a security protected area access command to an area in a security protected area and updating a verification key limited to that area, security intensity can be more enhanced.

[0057] According to the invention, an access-enabling setting that is necessary for access to a area with non-tamper resistance and verification key sharing are performed by the discretion of a area with tamper-resistance, and read and write of data are performed using commands suitable for a large capacity area, whereby both flexibility of security and read and write performance can be achieved.

Advantageous Effect of the Invention

[0058] According to the present invention, by dividing a command for access area designation and a command for security protection area access, and adding verification data to the command for security protection area access, a card can verify the identity of a terminal application having specified the access area, a terminal application having issued the command for security protection area access, and a terminal application that holds a verification key shared with the memory card, i.e., having

right to access the security protected area. Furthermore, regarding memory access, by using a two-stage command constitution, i.e., a command for access area designation and a command for security protection area access, while command complexity is avoided by using conventional memory card commands, even with only few command argument, without reducing security, access to the security protected area is enabled.

[0176] In the present embodiment, a session key sharing step is included in FIG.11. However, if it is considered that there is no need to update a session key each time as security policy, terminal 200 and card 100 may have in advance a verification key and an encryption key and may use the keys as a session key.